

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-300560

(43)Date of publication of application : 11.10.2002

(51)Int.Cl.

H04N 7/16

H04H 1/00

H04L 9/08

(21)Application number : 2001-101420

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 30.03.2001

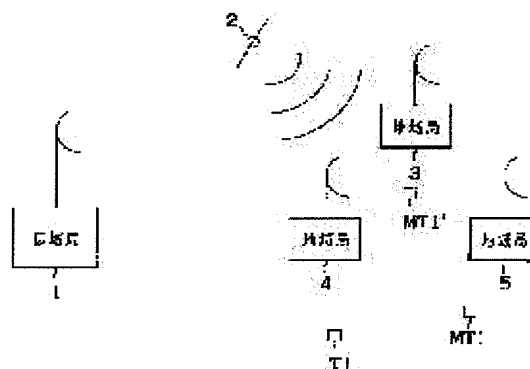
(72)Inventor : AKIYAMA KOICHIRO

(54) LIMITED RECEPTION SYSTEM, WIDE-AREA STATION CONTRACT CONTROLLER, AND LOCAL STATION CONTRACT CONTROLLER

(57)Abstract:

PROBLEM TO BE SOLVED: To reduce the quantity of transmission of limited reception information.

SOLUTION: A wide-area station 1 broadcasts the broadcast contents and the information relevant to programs by wide area broadcasting, which performs broadcasting over a relatively wide range. Moreover, the wide-area station 1 broadcasts information, relevant to channel contract having described the contract conditions for each channel for performing limited reception, for local stations 3, 4, and so on. The local stations 3, 4, and so on broadcast this information within their own broadcast ranges, when they receive the information relevant to the channel contracts addressed to subscribers within own stations. Hereby, the increase of the quantity of broadcast is suppressed.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-300560
(P2002-300560A)

(43)公開日 平成14年10月11日(2002. 10. 11)

(51)Int.Cl. ⁷	識別記号	F I	テラート*(参考)
H 0 4 N 7/16		H 0 4 N 7/16	Z 5 C 0 6 4
H 0 4 H 1/00		H 0 4 H 1/00	U 5 J 1 0 4
			B
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B
			6 0 1 D
審査請求 未請求 請求項の数10 O L (全 19 頁) 最終頁に続く			

(21)出願番号 特願2001-101420(P2001-101420)

(22)出願日 平成13年3月30日(2001. 3. 30)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 秋山 浩一郎

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(74)代理人 100076233

弁理士 伊藤 進

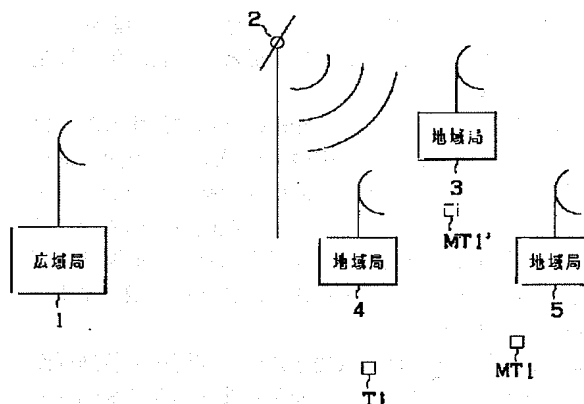
最終頁に続く

(54)【発明の名称】 限定受信システム、広域局契約管理装置及び地域局契約管理装置

(57)【要約】

【課題】限定受信情報の送信量を低減する。

【解決手段】広域局1は、放送コンテンツ及び番組関連情報については比較的広範囲に放送を行なう広域放送によって放送する。また、広域局1は、限定受信を行なうためにチャンネル毎の契約状態を記述したチャンネル契約関連情報については、地域局3, 4, …宛に放送する。地域局3, 4, …は、自局内の加入者宛チャンネル契約関連情報を受信すると、この情報を自局の放送範囲内に地域放送する。これにより、送信量の増大が抑制される。



【特許請求の範囲】

【請求項1】 コンテンツ情報を放送する広域放送局と、
前記コンテンツ情報を利用する契約した受信端末と、
前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報を、前記広域放送局の放送範囲よりも狭い放送範囲に放送する地域放送局とを具備したことを特徴とする限定受信システム。

【請求項2】 前記地域放送局は、地方局、中継局又はギャップフィルアーであることを特徴とする請求項1に記載の限定受信システム。

【請求項3】 前記地域放送局は、前記広域放送局が放送した契約関連情報を受信して、自放送範囲内に加入している前記受信端末に放送することを特徴とする請求項1に記載の限定受信システム。

【請求項4】 前記地域放送局は、前記広域放送局が通信によって送信した契約関連情報を受信して、自放送範囲内に加入している前記受信端末に放送することを特徴とする請求項1に記載の限定受信システム。

【請求項5】 契約した受信端末の利用に供するためにコンテンツ情報を放送する広域放送手段と、
前記広域放送手段の放送範囲よりも狭い放送範囲に放送する複数の地域放送局に対して、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報を、宛先を指定して送信する契約関連情報送信手段と具備したことを特徴とする広域局契約管理装置。

【請求項6】 前記契約関連情報送信手段は、前記複数の地域放送局に対して、放送又は通信によって前記契約関連情報を送信することを特徴とする請求項5に記載の広域局契約管理装置。

【請求項7】 前記地域放送局は、地方局、中継局又はギャップフィルアーであることを特徴とする請求項5に記載の広域局契約管理装置。

【請求項8】 契約した受信端末の利用に供するためにコンテンツ情報を放送する広域放送局から、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報が与えられ、前記広域放送局の放送範囲よりも狭い放送範囲に前記受信端末毎の契約関連情報を放送する地域放送手段を具備したことを特徴とする地域局契約管理装置。

【請求項9】 前記地域放送手段は、前記広域放送局から、放送又は通信によって前記契約関連情報を受信することを特徴とする請求項8に記載の地域局契約管理装置。

【請求項10】 前記地域放送手段は、地方局、中継局又はギャップフィルアーであることを特徴とする請求項8に記載の地域局契約管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、たとえば、契約内

容に応じて放送配信されるコンテンツを復号する有料放送サービスの契約関連情報の送信を効率化した限定受信システム、広域局契約管理装置及び地域局契約管理装置に関する。

【0002】

【従来の技術】近年、放送のデジタル化が進んでいる。通信衛星（CS）に始まり、ケーブルTV、地上放送へと進んだデジタル放送は、一層のサービスの充実とともに、これからの放送サービスの主役をつとめていくものと思われる。

【0003】デジタル放送の最大の特徴は、情報圧縮技術の導入によって番組の送信に要する周波数の使用効率が向上し、アナログ放送に比較して放送チャンネル数が大幅に増加したことである。更に、デジタル放送では、高度な誤り訂正技術を適用することができ、高品質で均質なサービスの提供が可能となる。

【0004】また、デジタル化によって、従来のような画像や音声による放送だけでなく、文字やデータによる放送（データ放送）も可能になり、例えばニュースを文字データとして放送することや、PC（パーソナルコンピュータ）ソフトを放送で配信することも可能となり、これらのサービスを提供するためのシステムも続々登場してきている。

【0005】ところで、有料放送サービスでは、番組の不正視聴を防止するために番組にスクランブルが施される。スクランブルを利用した有料放送では、契約内容に基づいたスクランブルの解除及び復号が受信機で可能なように、契約期間に即した顧客管理を行う必要がある。契約期間に即した顧客管理によって、例えば、所定の料金の支払による契約期間内に限って契約チャンネルの番組の視聴を許可することが可能となる。

【0006】不正視聴を防止する点から、受信装置にてスクランブルあるいは暗号を解くための鍵情報（限定受信情報）は、正当な視聴者のみに、契約チャンネル、契約期間に即して、確実に提供されるようにする必要がある。

【0007】図34はデジタル放送において採用される鍵構成の一例を示す説明図である。図34に示すマスター鍵KMは、放送受信装置に固有の鍵である。送信側では、図34の矢印に示すように、チャンネルキーKchを用いて放送コンテンツをスクランブルする。そして、各チャンネルに固有のワーク鍵Kwを用いて、スクランブルされた放送コンテンツ及びチャンネルキーKchを暗号化して送信する。

【0008】一方、ワーク鍵Kwは、マスター鍵KMによってチャンネル契約関連情報と共に暗号化されて送信される。チャンネル契約関連情報はチャンネル毎の契約期間又は契約の有無等の情報である。なお、ワーク鍵Kwは、契約最小期間（例えば1ヶ月）毎に更新される。

【0009】ワーク鍵Kw及びチャンネル契約関連情報

は、受信側において、コンテンツの受信に先だって受信されて蓄積される。コンテンツ視聴時はチャンネル契約関連情報を参照して、チャンネルの視聴可否を判断し、ワーク鍵Kwを用いて受信チャンネルのチャンネルキーKchを復号する。チャンネルキーKchによって、スクランブルされた放送コンテンツをデスクランブルする。

【0010】このように、図34の鍵構成を採用するデジタル放送方式では、有料放送の実現のために、契約者毎にチャンネル契約関連情報と該チャンネル契約関連情報に見合ったチャンネルのワーク鍵Kwを定期的に送信している。しかし、契約最小期間毎に契約者個別にワーク鍵を送信しなければならず、契約者の増加等によって、このような限定受信情報の送信量も増大し、その送信は困難になりつつある。

【0011】

【発明が解決しようとする課題】このように、従来、有料放送等の限定受信システムを可能にするためには、復号に用いるワーク鍵を定期的に放送する必要がある、契約者の増加等によって送信量が増大してしまうという問題点があった。

【0012】本発明はかかる問題点を鑑みてなされたものであって、限定受信に必要な情報の放送を効率化することにより、送信量の増大を抑制することができる限定受信システム、広域局契約管理装置及び地域局契約管理装置を提供することを目的とする。

【0013】

【課題を解決するための手段】本発明の請求項1に係る限定受信システムは、コンテンツ情報を放送する広域放送局と、前記コンテンツ情報を利用する契約した受信端末と、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報を、前記広域放送局の放送範囲よりも狭い放送範囲に放送する地域放送局とを具備したものであり、本発明の請求項5に係る広域局契約管理装置は、契約した受信端末の利用に供するためにコンテンツ情報を放送する広域放送手段と、前記広域放送手段の放送範囲よりも狭い放送範囲に放送する複数の地域放送局に対して、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報を、宛先を指定して送信する契約関連情報送信手段と具備したものであり、本発明の請求項8に係る地域局契約管理装置は、契約した受信端末の利用に供するためにコンテンツ情報を放送する広域放送局から、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報が与えられ、前記広域放送局の放送範囲よりも狭い放送範囲に前記受信端末毎の契約関連情報を放送する地域放送手段を具備したものである。

【0014】本発明の請求項1において、広域放送局は、コンテンツ情報を放送する。コンテンツ情報の利用を制御するために受信端末毎の契約関連情報は、広域放送局の放送範囲よりも狭い放送範囲に放送する地域放送

局によって放送される。受信端末は地域放送局の放送によって契約関連情報を受信し、これにより、受信端末は、コンテンツ情報を受信して利用する。

【0015】本発明の請求項5において、広域放送手段は、契約した受信端末の利用に供するためにコンテンツ情報を放送する。契約関連情報送信手段は、広域放送手段の放送範囲よりも狭い放送範囲に放送を行う複数の地域放送局に対して各宛先を指定して、コンテンツ情報の利用を制御するために受信端末毎の契約関連情報を送信する。

【0016】本発明の請求項8において、地域放送手段は、広域放送局から、コンテンツ情報の利用を制御するための受信端末毎の契約関連情報が与えられて、広域放送局の放送範囲よりも狭い放送範囲に受信端末毎の契約関連情報を放送する。

【0017】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。図1は本発明に係る限定受信システムの一実施の形態を示す説明図である。本実施の形態は受信機の固有のマスター鍵を用いる限定受信システムに適用したものである。

【0018】本実施の形態は衛星放送等を使って比較的広範囲に放送を行なう広域放送によって放送コンテンツを放送すると共に、チャンネル毎の契約状態を記述したチャンネル契約関連情報については、地上波等を使って比較的狭い範囲に放送を行なう地方放送等の地域放送によって放送することを可能にすることにより、送信量の増大を抑制するようにしたものである。

【0019】先ず、図2乃至図6を参照して、限定受信システムにおいて伝送される情報について説明する。

【0020】本実施の形態においては、各受信装置が個別のマスター鍵を有する場合の例を示している。即ち、本実施の形態では、図34と同様の鍵構成が採用される。

【0021】上述したように、このシステムでは、各受信装置に対して、定期的にしかも個別にチャンネル契約関連情報を暗号化して送信する必要がある、送信量が増大する。しかしその反面、マスター鍵が不正入手された場合の被害範囲が狭く安全性が高い。なお、以下に述べる限定受信方式は、社団法人電波産業会が策定したBSデジタル放送限定受信方式の標準規格のARIB STD-B25 1.0版（以下、ARIB規格という）に則った方式を簡明に説明したものである。

【0022】放送局が放送する放送コンテンツは、チャンネルキーKchを使って慣用暗号方式で暗号化される。更に、スクランブルされた放送コンテンツ及びチャンネルキーKchは、各チャンネルに固有のワーク鍵Kwを用いて暗号化される。

【0023】チャンネルキーKchは解読を防ぐため通常10分程度の短時間で変更する必要がある。従って、チャ

ネルキーKchを個別のマスター鍵を用いて暗号化すると、送信量が膨大となる。そこで、全受信装置に共通のワーク鍵KwでチャンネルキーKchを暗号化するのである。

【0024】また、同一のワーク鍵Kwを何カ月もの期間連続して使用すると、不正に解読される虞が高くなる。そこで、不正視聴を防止するために、視聴契約の変更時だけでなく適宜のタイミングでワーク鍵Kwを変更するようになっている。このため、放送コンテンツの復号に必要なワーク鍵Kwについても、多重化して受信側に送信する。この場合、ワーク鍵Kchについては受信機に固有のマスター鍵KMで暗号化して送信する。例えばマスター鍵KMが不正に入手された場合でも、ワーク鍵Kwを変更することによって無料視聴を防止することができる。

【0025】本実施の形態の限定受信システムにおいて放送受信装置が受信するデータは、コンテンツパケット、番組関連情報パケット、契約関連情報パケットの3種類である。

【0026】図2乃至図4は夫々コンテンツパケット、番組関連情報パケット及び契約関連情報パケットのパケット形式を示す説明図である。図2乃至図4において[]で囲ったデータは、スクランブル又は暗号化されたデータを示している。

【0027】図2に示すように、コンテンツパケットは、情報識別子、チャンネル識別子、チャンネルキー識別子、放送コンテンツによって構成される。情報識別子は、当該パケットの種別を示すもので、コンテンツパケットであることを示す識別子が記述される。チャンネル識別子は、当該放送コンテンツがいずれのチャンネルのコンテンツであるかを示すものである。

【0028】また、チャンネルキー識別子は、当該放送コンテンツを復号するチャンネルキーKchの識別子を示す。放送コンテンツは生の番組データで、チャンネルキー識別子で指定されたチャンネルキーKchで暗号化されている。なお、本実施の形態ではこれら全ての情報は固定長で表現されたデータであるものとする。

【0029】図3に示すように、番組関連情報パケットは、情報識別子、チャンネル識別子、ワーク鍵識別子、チャンネルキー識別子、チャンネルキーKchによって構成される。情報識別子は当該パケットの種別を示すもので、番組関連情報パケットであることを示す識別子が記述される。

【0030】チャンネル識別子は当該番組関連情報がいずれのチャンネルのものかを示すものである。また、ワーク鍵識別子は当該番組関連情報パケットがいずれのワーク鍵Kwによって暗号化されているかを示す情報である。チャンネルキー識別子は次に記述されているチャンネルキーの識別子であり、チャンネルキーKchはチャンネル識別子で指定されているチャンネルの放送コンテンツの暗号化に使

われているチャンネルキーKchを示している。本実施の形態ではこれら全ての情報は固定長で表現されたデータであり、チャンネルキー識別子からチャンネルキーKchまでのデータがワーク鍵識別子で指定されたワーク鍵で暗号化されている。

【0031】なお、図3の番組関連情報パケットは、上述したARIB規格におけるECM (Entitlement Control Message) に相当する。

【0032】図4に示すように、契約関連情報パケットは、情報識別子、受信装置ID、ワーク鍵情報、チャンネル契約関連情報C、誤り検出コードによって構成されている。情報識別子は当該パケットの種別を示すもので、契約関連情報パケットであることを示す識別子が記述される。受信装置IDは当該契約関連情報がいずれの受信装置宛てのものであるかを示すものである。

【0033】ワーク鍵情報は、当該受信者が契約しているチャンネルのワーク鍵についての情報である。図5はワーク鍵情報の形式を示す説明図である。図5に示すように、ワーク鍵情報は、ワーク鍵の数nとそれに続くn個のチャンネル識別子、ワーク鍵識別子、ワーク鍵の組で構成されている。

【0034】チャンネル契約関連情報Cは当該契約受信装置の契約状態を示すチャンネル契約関連情報である。図6のビット列はチャンネル契約関連情報を示している。チャンネル契約関連情報は、限定受信を行なうためチャンネル毎の契約状態を記述したものである。例えば、各チャンネルにチャンネル番号を付け、図6に示すように、チャンネル番号に対応したビット（契約フラグ）が“1”であるか否かによってチャンネルの契約状態を示している。図6の例では、契約フラグが“1”である第2、第5、第7、第8チャンネルが契約済であることを示している。

【0035】誤り検出コードはチャンネル契約関連情報の誤りを検出するためのコードである。本実施の形態では契約関連情報パケット中の全ての情報は固定長で表現されたデータであり、ワーク鍵情報から誤り検出コードまでが受信装置IDに対応した受信装置のマスター鍵で暗号化されている。

【0036】なお、図4の契約関連情報パケットは、上述したARIB規格におけるEMM (Entitlement Management Message) に相当する。

【0037】本実施の形態においては、図2のコンテンツパケット及び図3の番組関連情報パケットについては広域放送を行う広域局によって放送し、図4の契約関連情報パケットについては地域放送を行う地方放送局等の地域局によって放送するようになっている。

【0038】なお、契約関連情報パケットについては比較的狭い範囲に放送を行なう放送局によって放送すればよく、地域局として、独自には番組制作を行なわない広域放送の再送信設備である中継局を採用して放送を行ってもよい。中継局の多くは、無人で運営されている。

【0039】近年、自動車向けのデジタル放送においては、ギャップフィルアーと呼ばれる中継局が採用される。モバイル受信装置に対して放送送信を行なうシステムにおいては、受信装置が移動することから、例えば都市部のビルの谷間等のような不感地域が生ずる。このため受信障害が起きるような地域のビルの屋上等にギャップフィルアーを設け、衛星又は通信放送によって送信された放送波をギャップフィルアーで受信し、当該地域向けに再送信するのである。本実施の形態においては、契約関連情報パケットの送信にギャップフィルアーを利用可能である。

【0040】次に、コンテンツパケット、番組関連情報パケット及び契約関連情報パケットを受信して、希望する番組の視聴を行う受信装置について説明する。図7は受信装置の全体構成を示すブロック図である。図8乃至図11は受信装置の作用を説明するためのフローチャートである。図8乃至図11において符号A～Cは処理の連結を示している。

【0041】図8は受信アルゴリズムを示すフローチャートである。受信装置11は、受信信号をデスクランブルするデスクランブラを有していると共に、デスクランブルに必要なスクランブル鍵を発生するための限定受信チップ17を備えている。限定受信チップ17は、受信装置11内部で限定受信の仕組みを実現するハードウェアであり、限定受信のための秘密情報が含まれているので内部のメモリやハード構成に関して外部から容易に読み出し、書き込み又は変更が不能な耐タンパ構造を有しているものとする。

【0042】受信装置11は、図8のステップS1で、受信部12によって放送波を受信する。A/D変換部13は受信した放送波をA/D変換してデジタルデータに変換する(ステップS2)。デジタルデータは誤り検出/訂正部14に与えられて誤り検出/訂正が行われた後(ステップS3)、チャンネル選択部15に供給される。

【0043】チャンネル選択部15は、受信した放送パケットの情報識別子を参照して、各パケットがコンテンツパケット、番組関連情報パケット又は契約関連情報パケットのいずれであるかを判別する(ステップS4)。

【0044】受信パケットがコンテンツパケットである場合には、処理をステップS5に移行し、現在視聴中のチャンネルをチャンネルI/F(インタフェース)16を介して得て(ステップS5)、チャンネル選択部15で視聴チャンネルのみ限定受信チップ17のフィルタ部18に送信する。フィルタ部18はコンテンツパケットをデスクランブル部19に出力する(ステップS6)。

【0045】受信データが番組関連情報パケットである場合には、ステップS7からステップS8に処理を移行して、チャンネル選択部15を介して取込まれた番組関連情報パケットは、フィルタ部18によって番組関連情報復号部26に供給されて、復号が開始される。

【0046】受信データが契約関連情報パケットである場合には、ステップS9からステップS10に処理を移行して、チャンネル選択部15からの受信パケットは、フィルタ部18によって契約関連情報認証部21に供給される。契約関連情報認証部21によって、パケット内に含まれる受信装置IDが抽出され、受信装置ID格納部22から取り出した受信装置IDと比較することにより、当該契約関連情報パケットが自受信装置向けのものであるか否かを判定する。

【0047】受信した契約関連情報パケットが自受信装置宛ての契約関連情報である場合には、このパケットは契約情報復号部24に供給され、そうでなければ処理を終了する。

【0048】契約関連情報パケットには受信装置個別のマスター鍵によって暗号化されている部分があることから、復号に先だって自受信装置宛てのパケットであるか否かを判定する必要がある。

【0049】次に、図9のフローチャートを参照して、コンテンツパケットに間する処理について説明する。デスクランブル部19は、図9のステップS11において、フィルタ部18から供給されたコンテンツパケットのチャンネル識別子とチャンネルキー識別子とをチャンネルキー出力部28に送信して、チャンネルキー出力部28に対してチャンネルキーKchの出力を要請する。

【0050】チャンネルキー出力部28は契約判定部30にチャンネル識別子を送り、チャンネルキーKchの出力の可否を問い合わせる(ステップS12)。契約判定部30ではこれを受けて、チャンネル契約情報格納部29からチャンネル契約関連情報を引き出し(ステップS13)、契約フラグが“1”であれば許可(ステップS16)、“0”であれば不許可の信号(ステップS20)をチャンネルキー出力部28に出力する。

【0051】チャンネルキー出力部28では送られてきた判定が許可であればチャンネルキー格納部27から当該チャンネルのチャンネルキー識別子を保持したチャンネルキーKchを得てデスクランブル部19に送信し(ステップS17)、不許可であればコンテンツパケットに関する処理を終了する。

【0052】なお、ここでコンテンツパケットはパケットの中でも最も多いのでパケット毎に同様の処理を繰り返すと処理に長時間を要する。そこで、同一チャンネルの同一チャンネルキーKchを用いている限りは、一回チャンネルキーKchの出力が許可された場合には、毎回契約判定部30に問い合わせることなくチャンネルキーKchを出力することにより、処理時間を短縮するようになっている。実際には、チャンネルキーKchはセキュリティ上の理由で10秒に1回程度の割合で変更されることから、出力可否の問い合わせを省略しても、限定受信に与える影響は少ない。

【0053】デスクランブル部19ではチャンネルキー

Kchの出力を受けて、コンテンツパケットの暗号化部分を復号し(ステップS18)、コンテンツ出力部20に出力する(ステップS19)。コンテンツ出力部20はコンテンツをモニタ等の再生装置に出力して再生させる。

【0054】受信情報が番組関連情報パケットであった場合には、図8のステップS8 から図10のステップS21に処理を移行する。番組関連情報復号部26はフィルター部18から番組関連情報パケットをが与えられると、チャンネル識別子とワーク鍵識別子をキーにして、対応するワーク鍵Kwをワーク鍵格納部25から取得する。

【0055】ここで対応するワーク鍵Kwが無い場合には、処理を終了する。ワーク鍵Kwを取得すると、番組関連情報復号部26は、取得したワーク鍵Kwを用いて番組関連情報を復号する(ステップS22)。復号された番組関連情報の中からチャンネルキーKchとそのチャンネル識別子を取り出し(ステップS23)、チャンネルキー格納部27へ格納する(ステップS24)。

【0056】受信情報が契約関連情報であった場合には、図8のステップS10から図11のステップS31に処理を移行し、契約関連情報認証部21は、受信装置ID格納部22から受信装置IDを抽出する。(ステップS31)。契約関連情報認証部21は、抽出した受信装置IDと契約関連情報パケットに含まれる受信装置IDとを比較することにより、当該契約関連情報が自受信装置宛てのものであるか否かを判定する(ステップS32)。自受信装置宛てのものでなければ、その時点で処理を終了する。

【0057】自受信装置宛の契約関連情報を受信した場合には、契約関連情報認証部21は、契約関連情報を契約関連情報復号部24に出力する。契約関連情報復号部24は、装置個別に設定されているマスター鍵KMをマスター鍵格納部23から取得し(ステップS33)、契約関連情報パケットの暗号化部分を復号する(ステップS34)。契約関連情報復号部24は、復号した受信契約関連情報から誤り検出コードを取得し、取得した誤り検出コードを検証することにより当該チャンネル契約関連情報が正しいものであるか否かを確認する(ステップS35)。

【0058】ステップS35の検証処理によって、契約関連情報パケットの中で暗号化されていない受信装置IDを偽造して作成された偽の契約関連情報に基づいて処理が行われることを防止することができる。誤り検出コードは契約関連情報から導出されるものであり、契約関連情報を暗号化したまま改変して偽造しようとしても、復号した際、復号契約関連情報から導出された誤り検出コードと復号によって得られた誤り検出コードとが一致することは極めて稀であり、偽造を確実に防止することができる。なお、仮に誤り検出コードを用いない場合には、暗号化された契約関連情報を適当に改変することに

より、復号した結果が元の契約関連情報よりも受信者に有利な条件の契約関連情報に変更可能である可能性が高くなってしまう。

【0059】誤り検出コードが検証されると、処理をステップS36に移行して、契約関連情報復号部24は、契約関連情報パケットからワーク鍵Kwとチャンネル契約関連情報Cとを取得し(ステップS36、S38)、夫々ワーク鍵格納部25又は契約情報格納部29に格納する(ステップS37、S39)。

【0060】図1において、広域局1は、衛星2を利用して、広域放送を行う。衛星2は広域局1からの放送波を中継して各地域局3、4、…に送信する。各地域局3、4、…は、衛星2からの放送波を受信して、地域内に地域放送を行う。

【0061】受信端末T1及び移動受信端末MT1は、図7の受信装置によって構成される。図1の例では、受信端末T1は固定端末であり、地域局4の加入端末(登録された受信端末)である。また、移動受信端末MT1は、移動端末であり、地域局3、5の加入端末である。図1の移動受信端末MT1'は、移動受信端末MT1が移動したことを示している。

【0062】地域局3、4、…は、契約関連情報については、自放送地域内で登録された受信端末宛のみの放送波を受信して中継放送を行うようになっている。

【0063】即ち、本実施の形態は、衛星放送等の広域放送のみを利用して送信されていた個別受信装置に対する限定情報(契約関連情報)を、受信装置が存在する特定地域のみに向けて放送することにより、限定受信の情報送信量を削減するものである。

【0064】広域放送局1はコンテンツパケット及び番組関連情報パケットについては、全地域局で中継可能のように、通常の広域放送を行う。一方、契約関連情報パケットについては、各地域局を宛先にして放送を行う。このような契約関連情報の限定受信を可能にするために、広域放送局1は広域局契約管理装置を備えている。

【0065】図12は広域放送局1内に設けられた広域局契約管理装置40の具体的な構成を示すブロック図である。

【0066】契約内容情報入力部41は、各契約の内容に応じて、契約ユーザDB(データベース)42及び地域局DB43に情報を入力する。図13は図12中の契約ユーザDB42に蓄積されている情報のフォーマットを示し、図14は図12中の地域局DB43に蓄積されている情報のフォーマットを示し、図15は図12中のワーク鍵DB46に蓄積されている情報のフォーマットを示している。

【0067】契約ユーザDB42は、図13に示ように、受信装置ID、加入している地域局の地域局コードの数nとそれに続くn個の地域局コード、チャンネル契約関連情報を格納している。これらのレコードは当該受信

装置IDを持つ受信装置は地域局コード1～nまでの地域局域に存在し、チャンネル契約関連情報に示すようなチャンネル契約を行なっていることを示している。

【0068】地域局DB43は、図14に示ように、地域局コード、地域局電話番号、地域局域加入者数k、継続レコード番号からなるレコードを格納している。地域局電話番号は地域局に対して通信を利用する場合に利用する電話番号であり、本実施の形態のように衛星放送によって契約関連情報を送信する場合には、不要である。

【0069】加入者数kは当該地域局コードを含んでいる契約ユーザDB42内のレコードの数であり、継続レコード番号は当該地域局コードを含む契約ユーザDB42のレコードのうち直前に送信したレコードの次のレコードが表示される。継続レコード番号は、1日分の送信終了後に更新されるようになっている。

【0070】送信スケジュール部44は、地域局DB43から各地域局毎に地域局域加入者数kを取得する。そして、各地域局に対して、所定の期間、例えば1ヶ月(30日)で、各地域局の加入者全てに契約関連情報を送信するようにスケジュールを立てる。なお、地域局の加入者数(受信装置数)が少ない場合には、1ヶ月1回よりも頻繁に(例えば1週間に1回)契約関連情報を送信することができる。

【0071】送信スケジュール部44は、契約ユーザDB42から各契約ユーザの情報を読み出して契約関連情報生成部45に与え、契約関連情報生成部45は、ワーク鍵DB46の内容に従って契約関連情報を作成する。

【0072】ワーク鍵DBは、図15に示すように、チャンネル識別子、ワーク鍵識別子、ワーク鍵、有効期限の内容を含んでいる。ワーク鍵はワーク鍵識別子を識別子とするチャンネル識別子で示されるチャンネルのワーク鍵であり、有効期限に示す期間だけ有効であることを示している。

【0073】契約関連情報生成部45は、契約ユーザDB42から抽出したレコードから受信装置IDとチャンネル契約関連情報を抽出し、チャンネル契約関連情報の中で契約フラグが“1”であるチャンネルに対して送信すべきワーク鍵とその識別子及びチャンネル識別子をワーク鍵DB46から抽出する。ここで送信すべきワーク鍵とは通常現在有効であるワーク鍵と次に有効になるワーク鍵である。

【0074】契約関連情報生成部45は、地域局の加入者に送信すべき契約関連情報を地域局送信用契約関連情報生成部47に出力する。地域局送信用契約関連情報生成部47は、地域局送信用契約関連情報を作成する。

【0075】図16は地域局送信用契約関連情報を示す説明図である。図16に示すように、地域局送信用契約関連情報は、情報識別子、地域局コード、契約関連情報の数とその数分だけの契約関連情報によって構成されている。ここで、情報識別子は当該パケットが地域局送信

用契約関連情報であることを示しており、地域局コードは当該パケットがどの地域局宛てのものであるか否かを表している。更にその地域局域内にある複数の受信端末宛の契約関連情報が配列される。

【0076】地域局送信用契約関連情報生成部47によって生成された地域局送信用契約関連情報は、地域局送信用契約関連情報出力部48に与えられる。地域局送信用契約関連情報出力部48は、地域局送信用契約関連情報を衛星2を介して送信する。衛星2からの地域局送信用契約管理情報は、地域局3、4、…に設けられた地域局契約管理装置50によって受信される。

【0077】図17は図1中の地域局3、4、…に設けられる地域局契約管理装置50の具体的な構成を示すブロック図である。

【0078】地域局契約管理装置50の受信部51は、衛星からの放送を受信する。A/D変換部52は、受信部51の受信信号をA/D変換して、誤り検出/訂正部53に出力する。誤り検出/訂正部53は、誤り訂正又は検出を行なって、正常なデータのみをフィルタ部18に出力する。フィルタ部18は、当該受信パケットの情報識別子を参照して地域局送信用契約関連情報であるか否かを判定する。

【0079】フィルタ部54は、地域局コード格納部55に格納された自局の地域局コードとの比較によって、地域局送信用契約関連情報が自局向けのものであるか否かについても判定する。フィルタ部54は、自局向けの地域局送信用契約関連情報から契約関連情報を抽出して送信DB56に出力する。

【0080】送信DB56は、フィルタ部54からの契約関連情報を記憶する。送信DB56に登録されているレコードは登録されて1日以上経過すると消去されるようになっており、1日毎に契約管理装置から送信される契約関連情報は全て更新される。

【0081】送信スケジュール部44は、送信DB56に登録されている契約関連情報を所定のスケジュールに従って送出部58に出力して、地域放送の限定受信専用チャンネル若しくは広域放送の限定受信専用チャンネルの合間に暫時繰り返し放送される。

【0082】次に、このように構成された実施の形態の動作について図18乃至図20のフローチャートを参照して説明する。なお、番組関連情報及び放送コンテンツ情報の送信方法は従来と同様であり、説明を省略する。

【0083】広域局61内の送信スケジュール部44は、図18のステップS41において地域局を示すiを1に初期化した後、地域局DB43からi番目の地域局レコードを抽出する(ステップS42)。次に、送信スケジュール部44は、抽出した地域局レコードから地域局コードと地域局域加入者数kiを取得する(ステップS43)。更にki/30とMとの最大を取ってmとする(ステップS44)。Mは1日に最低限送信したい契約関

連情報の数である。即ち、 $k_i / 30$ は約1ヶ月(30日)で一回りするための1日分を意味している。

【0084】従って、この m を取ることによって、最低限1ヶ月でその地域にある受信装置に送信することを意味している。もちろん当該地域に存在する受信装置が少なければ1ヶ月1回よりも頻繁に(例えば1週間に1回)送信することができる。なお、これらの数値 M 、30は利用形態によって様々に変更されるべきものである。

【0085】次に、送信スケジュール部44は、継続レコード番号(図14)をレコードから抽出し、継続レコード番号に従って、最大 m 個の地域局コードがついたレコードを契約ユーザDB42から抽出する(ステップS45)。ここで、継続レコードが契約ユーザDB42の範囲外となった場合には、自動的に契約ユーザDB42の先頭に戻って抽出を継続する。

【0086】本実施の形態における継続レコード番号とは、当該地域コードに対応する地域局に対して、当日送信を開始するレコード番号であり、前日に当該地域局に送信したレコードのうち、契約ユーザDB42上で最後にあたるレコードの次のレコードである。

【0087】送信スケジュール部44は、最大 m 個のレコードを抽出すると、ステップS46において $j = 1$ とし、 j 番目のレコード(登録した受信端末(装置)のレコード)があるか否かを確認する(ステップS47)。 j 番目のレコードが存在する場合には、ステップS48において、契約関連情報生成部45は、 j 番目のレコードから図19のアルゴリズムによって契約関連情報を作成する。

【0088】即ち、契約関連情報生成部45は、図19のステップS61、S62において、図13に示す契約ユーザDB42から抽出したレコードから受信装置IDとチャネル契約関連情報を抽出し、チャネル契約関連情報の中で契約フラグが“1”であるチャネルに対して送信すべきワーク鍵とその識別子及びチャネル識別子をワーク鍵DB46から抽出する(ステップS63、S64)。ここで送信すべきワーク鍵とは通常現在有効であるワーク鍵と次に有効になるワーク鍵である。これらはワーク鍵DB46の有効期限情報で知ることができる。

【0089】例えば、 i 番目の地域局が図1の地域局5を示すもので、 j 番目のレコードが受信端末MT1を示すものである場合には、この受信端末MT1に関する契約関連情報を生成する。

【0090】次に、 j をインクリメントして(ステップS49)、ステップS48、S48の処理を繰り返す。ステップS47において j 番目のレコードが無いことを検出すると、地域局コードを持つ地域局から送信すべき契約関連情報の作成が終了したので、次に地域局に送信するための準備に入る。即ち、ステップS50において $j = 0$ でないことを確認した後、ステップS51において地域局送信

用契約関連情報を作成する。

【0091】地域局送信用契約関連情報生成部47は、図16に示す地域局送信用契約関連情報を作成する。地域局送信用契約関連情報は、図16に示すように、情報識別子、地域局コード、契約関連情報の数とその数分だけの契約関連情報によって構成されている。ここで、情報識別子は当該パケットが地域局送信用契約関連情報であることを示しており、地域局コードは当該パケットがどの地域局宛てのものであるか否かを表している。更にその地域局域内にある受信装置の契約関連情報がその総数の後に続く。

【0092】地域局送信用契約関連情報生成部47によって生成された地域局送信用契約関連情報は、次のステップS52において、地域局送信用契約関連情報出力部48から送信される。なお、ステップS50の判断時に $j = 0$ である場合には、 i 番目の地域局域内には受信装置が存在しないことを意味するので送信のための処理を行わず、 $i = i + 1$ として次の地域局の処理に移る(ステップS53)。

【0093】こうして、図1の各地域局3、4、…の受信端末T1、MT1(MT1')についての契約関連情報も、これらの端末を加入者とする地域局宛に図16の地域局送信用契約関連情報の放送が行われる。

【0094】 i 番目の地域局送信用契約関連情報の送信が終了したら、 N を地域局の総数として $i = i + 1$ として $i < N$ であるか否かを判断する(ステップS54)。 $i < N$ であれば次の地域局域内の受信装置に関して同様の操作を繰り返す。 $i \geq N$ の場合には、地域局DB43に登録されている地域局に関して、1日分の送信操作が終了したことになるので、図18のフローを終了し、翌日また起動する。

【0095】一方、地域局3、4、…においては、地域局契約管理装置50の受信部51において、衛星からの放送を受信する(図20のステップS71)。A/D変換部52は、受信部51の受信信号をA/D変換して(ステップS72)誤り検出/訂正部53に出力する。誤り検出/訂正部53は、誤り訂正又は検出を行なって(ステップS73)、正常なデータのみをフィルター部18に出力する。フィルター部18は、当該受信パケットの情報識別子を参照して地域局送信用契約関連情報であるか否かを判定する(ステップS74)。

【0096】地域局送信用契約関連情報でなかった時は、そのパケットの処理を終了する。地域局送信用契約関連情報であった場合には、ステップS75において、自局向けのものであるか否かを判定する。自局向けでなければ処理を終了する。自局向けであれば、当該パケットに含まれている契約関連情報を抽出して、送信DB56に登録する(ステップS76)。

【0097】ここで送信DB56に登録されているレコードは登録されて1日以上経過すると消去されるように

構成されている。このため、1日毎に契約管理装置から送信される契約関連情報が全て更新される。

【0098】送信DB56に登録されている契約関連情報は、送信スケジュール部57によって指示されたスケジュールに従って地域放送の限定受信専用チャンネル若しくは広域放送の限定受信専用チャンネルの合間に暫時繰り返し放送される。(ステップS77)。

【0099】こうして、受信端末T1は地域局4から放送された契約関連情報を受信し、移動受信端末MT1、(MT1')は地域局5、3から契約関連情報を受信する。1受信端末であっても複数の地域局に登録することによって、登録した複数の地域局から契約関連情報を取得することができ、移動端末であっても、登録した地域局の放送範囲内であれば、限定受信が可能である。

【0100】このように、本実施の形態においては、各受信機が受信すべき番組関連情報、放送コンテンツ情報及び契約関連情報のうち、限定受信の対象となる契約関連情報については、対応する地域局のみから送信するようになっている。これにより、契約関連情報の送信量を削減することができる。

【0101】契約関連情報の送信量の削減により、同じ帯域幅であれば各契約者に対する契約関連情報の送信頻度を上げることができる。このことは例えば前述したモバイル放送の場合特に有効である。何故ならモバイル放送における受信装置は(車庫に入ったり等して)常に受信状態にあるとは言えない。このため受信情報になった再、タイムリーに契約関連情報を受信することができる本発明は有用である。

【0102】図1の実施の形態においては、広域局が衛星を利用して契約関連情報を地域局に送信する例について説明した。広域局から地域局への契約関連情報の送信に、通信を利用することも考えられる。

【0103】図21はこの場合の実施の形態を示す説明図であり、契約関連情報を広域局から地域局に通信を利用して送信する例を示している。図21において、広域局61は、図示しない衛星等を利用して広域放送を行うと共に、限定受信情報については、地域局62、63、…に対して所定の通信路を介した通信が可能である。各地域局62、63、…は、衛星等から広域放送の放送波を受信して地域内に地域放送を行うと共に、通信路を介して通信によって限定受信情報を受信して、地域内に地域放送を行うことができるようになっている。

【0104】ところで、地域局62、63、…へのデータの送信は、地域局の電話番号とプロトコルさえ知っていればだれでも可能である。従って、善意悪意に拘わらず誤ったデータが地域局62、63、…に送信されて、そのまま放送されてしまう危険がある。

【0105】このため、地域局62、63、…は、公衆通信網を利用した契約関連情報の送受信において、受信したデータが確かに広域局から送られてきたものか否か

を確認する必要がある。そこで、本実施の形態では、広域局61から地域局62、63、…に送信データを送る際に、データにデジタル署名を付加し、地域局62、63、…が広域局61から該送信データを受信する際に付随しているデジタル署名を検証することによって、広域局61からのデータであることを確認するようになっている。

【0106】図22は図21中の広域局61に設けられる広域局契約管理装置71の具体的な構成を示すブロック図である。図22において図12と同一の構成要素には同一符号を付して説明を省略する。

【0107】図22の広域局契約管理装置71は、地域局送信用契約関連情報生成部47に署名生成鍵格納部72が付随する点が図12の広域局契約管理装置40と異なる。署名生成鍵格納部72は、署名生成鍵を格納しており、地域局送信用契約関連情報生成部47は、地域局送信用契約関連情報を生成する際に図16に示す地域局送信用契約関連情報の契約関連情報の数から契約関連情報までの部分について、署名生成鍵格納部72に格納されている署名生成鍵によってデジタル署名を作成するようになっている。地域局送信用契約関連情報生成部47は、図23に示すように、地域局送信用契約関連情報の最後に、作成したデジタル署名を付加して地域局送信用契約関連情報出力部48に出力する。

【0108】図24は図21中の地域局62、63、…に設けられる地域局契約管理装置81の具体的な構成を示すブロック図である。図24において図17と同一の構成要素には同一符号を付して説明を省略する。

【0109】モデム部82は、通信路を介して伝送された情報を受信して、地域局コード検証部83に出力する。地域局コード格納部55には自地域局のコードが格納されている。地域局コード検証部83は、受信した情報中の地域局コードと地域局コード格納部55に格納されている地域局コードとが一致することによって自局宛の情報であるものと判断する。

【0110】地域局コード検証部83は、受信情報を署名検証部85に出力する。署名検証鍵格納部86は、署名検証鍵を格納しており、署名検証部85は、受信情報に含まれるデジタル署名を署名検証鍵で検証することによって署名検証を行う。正しく署名検証された場合にのみ、署名検証部85は受信データの契約関連情報を送信DB56に出力するようになっている。

【0111】次に、このように構成された実施の形態の動作について図25のフローチャートを参照して説明する。図25において図20と同一の手順には同一符号を付して説明を省略する。

【0112】広域局61の広域局契約管理装置71は、地域局送信用契約関連情報を生成する場合には、地域局送信用契約関連情報の契約関連情報の数から契約関連情報までの部分について署名生成鍵格納部72に格納され

ている署名生成鍵によってデジタル署名を作成し、地域局送信用契約関連情報の最後に付加して出力する。他の作用は図12の広域局契約管理装置40と同様である。

【0113】一方、地域局契約管理装置81においては、モデム部82において公衆回線からの情報を受信する(ステップS71)。受信された情報は地域局送信用契約関連情報であることが確認された後(ステップS74)、地域局コード検証部83に供給される。受信された情報が地域局送信用契約関連情報ではなかった場合には当該情報に関する処理を終了する。

【0114】地域局コード検証部83は地域局送信用契約関連情報パケットに含まれる地域局コードが自局のものか否かをチェックする(ステップS75)。地域局コードが自局のものでなければ処理を終了し、自局のものであれば、当該パケットを署名検証部85に出力する。署名検証部85では、デジタル署名の検証が行なわれる(ステップS81)。署名検証に失敗した場合には処理を終了する。デジタル署名が検証された場合には、パケットの中から契約関連情報の数だけ契約関連情報を抽出し、送信DB56に登録する(ステップS76)。送信DB56に登録されている契約関連情報は放送スケジュール部57からのスケジュールに従って地域放送の限定受信専用チャンネル若しくは広域放送の限定受信専用チャンネルの合間に暫時繰返し放送される。(ステップS77)。

【0115】このように、本実施の形態においても図1の実施の形態と同様の効果を得ることができる。

【0116】なお、上記図1の実施の形態においては、広域局から地域局に衛星放送によって地域局送信用契約関連情報を送信する場合にはデジタル署名の生成及び検証を行っていないが、図21の実施の形態と同様の構成によって、デジタル署名を導入することができることは明らかである。この場合には、衛星放送による地域局送信用契約関連情報の送信をより確実なものにすることができる。

【0117】また、逆に、広域局と地域局の間に専用線が設けられていること等によって他から通信される恐れがない場合には、通信による送信であってもデジタル署名の必要はない。このように上記各実施の形態は利用形態によって様々変更可能である。

【0118】また、広域局から地域局への送信をより確実にするためには、衛星放送による送信と通信による送信とを併用するシステムが望ましい。このような構成は、図1及び図21において、広域局にあっては送信部を、地域局にあっては受信部を2つ備えることによって可能であり、処理の流れも2つの場合に分けてそれぞれ上述した処理を行なうことによって容易に構成することができる。

【0119】また、上記各実施の形態における地域局としては人的介入が全くなく全て自動的に行なうよう構成

することができることから、地域向けの番組を放送する局ばかりでなく、単に電波増幅のための中継局であってもよい。即ち、中継局としてはモバイル放送等で利用されるギャップフィラーでも構わないし、地域局として移動局を採用することも可能である。このように本実施の形態では地域局として(無人有人の別なく)地域放送システムを利用することが可能である。

【0120】また、上記各実施の形態では、各受信装置に対して契約関連情報を送信する地域局に関しては特に限定していなかったが、据え置き型の受信装置の場合は設置場所が局域に入るような地域局1局から送信すればよいが、車載受信装置のようなモバイル環境下にある受信装置に対しては複数の地域局から契約関連情報を送信する必要がある。このため、モバイル受信装置での受信を前提とした放送システムにおいては広域局側の契約管理装置の契約ユーザDBの地域局コードには複数の地域局コードが登録できるように構成するのが望ましい。更に、モバイル放送においては例えば高速道路を日夜走るトラックのように移動経路がはっきりしている受信装置向けに高速道路上にある地域局を全て束にして扱うように地域局コードを構成したり、地域局コードは別々でも処理の中で一括して送信するような工夫が望まれる。

【0121】また、地域局としてギャップフィラー等狭い範囲に対してのみ有効な中継局を利用すると地域の限定が強くなり、受信装置に対する契約関連情報の送信効率が上がる反面で、広域局から地域局送信用契約関連情報を送信する中継局の数が多くなり、広域局からの送信に長時間を要する等の不都合が生ずる。

【0122】そこで、図26に示す階層構造を利用する方法が考えられる。図26に示すように、地域局の中に親局92、93、…と子局A1～An、B1～Bm、C1～Cuを設け、広域局91からは親局92、93、…に対して、親局92、93、…の支配下にある子局A1～An、B1～Bm、C1～Cuに送信する契約関連情報を送信し、各親局92、93、…が支配下の子局A1～An、B1～Bm、C1～Cuに対して、それぞれのデータを送信するような構成をとることが望ましい。同様に子局A1～An、B1～Bm、C1～Cuが更に孫局に送信する場合も考えられ、この場合には一層効率を向上させることができる。このような構成における認証は、子局が広域局の認証を行なうような構成にしてもよく、また、直接親局を認証するように構成してもよい。特に、広域局と親局の間が専用線で接続され、認証の必要がない場合等には後者が有効となる。

【0123】また、図21の実施の形態では、通信で地域局送信用契約関連情報を送信する際、広域局から地域局に向けて通信しているが、この逆でも構わない。但し、この場合には、広域局はどこから電話が掛かってきたか分からないことがあるので、広域局が地域局を認証する必要がある。この場合の認証は、チャレンジ・レス

ポンス型の認証を用いればよい。更に、図21の実施の形態における地域局が広域局を認証する認証方式にもチャレンジ・レスポンス型の認証を行なうこともできる。

【0124】更に本実施の形態では、本発明の構成を明らかにするため契約関連情報を地域局から送信する場合のみを述べてきたが、これを現行の広域局からの送信と併用しても構成上矛盾は生じない。この場合2つの方式が考えられる。1つは広域局からの限定受信情報送信の合間に地域局からの契約関連情報の送信を挟む方式。もう1つは（広域局からの送信を前提とする）従来の限定受信チャンネルの他に地域放送から契約関連情報を送信するため限定受信チャンネルを創設し、後者のチャンネルで前記実施の形態で述べた方式で契約関連情報を送信する方式である。

【0125】また、このように広域放送による契約関連情報の送信と、地域放送による契約関連情報の送信を併用すると、引越しその他の理由により、受信装置の受信エリアが変更された場合でも、十分対応できるという利点がある。

【0126】図27乃至図33は本発明の他の実施の形態に係り、図27は鍵構成を示す説明図、図28は契約関連情報パケットを示す説明図、図29は契約関連情報を示す説明図、図30は受信装置の構成を示すブロック図、図31乃至図33は受信装置の動作を説明するためのフローチャートである。

【0127】図1及び図21の実施の形態においては、受信装置に固有のマスター鍵を用いる限定受信システムに適用した例であったが、本実施の形態は全ての受信装置が共通のマスター鍵を有する限定受信システムに適用した例である。本実施の形態のハード構成は、図1又は図21の実施の形態と同様であり、図示を省略する。

【0128】このような限定受信システムにおいては各受信装置に対して、個別に契約関連情報を暗号化して送信する必要がないので限定受信情報の送信量が少なくてすむという利点がある。しかし、マスター鍵が不正に取得された場合には被害範囲が大きいという安全性の問題を有する。そこで、デジタル署名等の偽造防止技術を用いて対策する必要がある。なお、以下に述べる方式は、電気通信技術審議会資料「2.6GHz帯の電波を利用する衛星デジタル音声放送システムの技術的条件」に基づく方式を簡明に説明したものである。

【0129】本実施の形態においては、図27に示すように、2段の鍵構成を採用する。即ち、放送コンテンツをチャンネルキーKchでスクランブルを施すと共に、チャンネルキーKchとチャンネル契約関連情報とを全ての受信装置に共通のマスター鍵KMで暗号化して送信する。送信されたチャンネルキーKchを用いて放送コンテンツを復号する。

【0130】本実施の形態の限定受信システムにおいて放送受信装置が受信するデータは、コンテンツパケット

及び契約関連情報パケットの2種類である。コンテンツパケットは、図3と同一の形式を有する。一方、契約関連情報パケットは図28に示す形式を有する。

【0131】即ち、コンテンツパケットは、図3に示すように、情報識別子、チャンネル識別子、チャンネルキー識別子、放送コンテンツによって構成されており、放送コンテンツはチャンネルキーKchによって暗号化されている。各情報の意味と役割は図1の実施の形態と同一である。

【0132】契約関連情報パケットは、図28に示すように、情報識別子、マスター鍵識別子、チャンネル識別子、チャンネルキー識別子、チャンネルキー、契約関連情報の数n、n個の契約関連情報及びデジタル署名によって構成されている。チャンネル識別子からデジタル署名までの部分はマスター鍵で暗号化される。デジタル署名は、契約関連情報数nから契約関連情報nまでの部分に関するデジタル署名である。デジタル署名は契約関連情報の偽造を防ぐためのものであり、契約関連情報を1ビットでも変更するとデジタル署名が検証できなくなるという性質を有する。また、デジタル署名を作成するには放送局側にしか存在しない秘密鍵を知る必要があり、デジタル署名を付加することによって契約関連情報の偽造を防止することができる。

【0133】契約関連情報は、図29に示すように、受信装置IDとチャンネル契約関連情報とから構成されており、受信装置IDに対応するチャンネル契約関連情報を表している。契約関連情報に含まれるその他の情報は、図1の実施の形態に示されている対応する情報と同一の意味と役割を有する。

【0134】このように構成された実施の形態においては、コンテンツパケットは各地域局において同一内容が広域に放送される。一方、契約関連情報パケットについては、各地域局の加入者宛に地域放送される。

【0135】図30は本実施の形態において採用される受信機の構成を示している。図30において図7と同一の構成要素には同一符号を付して説明を省略する。また、図31乃至図33において図8、図9及び図11と同一の手順には同一符号を付して説明を省略する。

【0136】図30の放送受信装置は、受信部12において放送波を受信後（図31のステップS1）、A/D変換部13にてA/D変換を行なって（ステップS2）デジタルデータに変換する。次に、ステップS3において、誤り検出／訂正部14は、誤り検出及び誤り訂正を行なう。フィルタ部18は、パケット内の情報識別子によってコンテンツパケットであるか否かを判断し（ステップS4）、そうであればチャンネル識別子を参照して、視聴チャンネルのコンテンツか否かを判定する（ステップS5）。視聴チャンネルであった場合には、ステップS6でコンテンツパケットはデスクランブル部19に供給される。そうでない場合には、当該パケットに関する

処理を終了する。契約関連情報パケットであった場合には、フィルター部18はステップS9からステップS10に処理を移行して、契約関連情報パケットを契約関連情報復号部24に供給する。

【0137】視聴チャンネルのコンテンツパケットの処理は、図1の実施の形態と同様である。契約関連情報パケットの処理は、図33のフローチャートに従って行われる。即ち、契約関連情報が契約関連情報復号部24に入力されると、契約関連情報復号部24はマスター鍵識別子をキーにして、マスター鍵格納部23からマスター鍵KMを取得して(ステップS33)、暗号化部分を復号する(ステップS34)。契約関連情報復号部24は、復号された契約関連情報からチャンネルキー、チャンネル識別子、チャンネルキー識別子を抽出し(ステップS90)、チャンネルキー格納部27に格納する(ステップS91)。

【0138】次に、契約関連情報復号部24は、契約関連情報数nからデジタル署名までの部分を契約情報認証部21に出力する。契約情報認証部21は契約関連情報数nを抽出し、それを変数MAXに代入する(ステップS92)。契約情報認証部21は、最後の契約関連情報の認証が終わるまで引き続き契約関連情報を次々参照する(ステップS94)。

【0139】契約情報認証部21は、ステップS95において契約関連情報が自装置宛のものであるか否かを判定し、自装置宛のものである場合には、デジタル署名を検出する(ステップS97)。契約関連情報復号部24は、デジタル署名を検証後に、対応するチャンネル契約関連情報Cを契約情報格納部29へ格納する(ステップS99)。自受信装置の受信装置IDと一致する契約関連情報がない場合やデジタル署名が検証できなかった場合には、当該パケットに関する処理を終了する。

【0140】このように、本実施の形態においても、図1及び図21の実施の形態と同様の効果を得ることができる。

【0141】本実施の形態の限定受信方式ではワーク鍵を用いておらずマスター鍵が共通であることから、解約等視聴しなくなるチャンネルが生じた場合には受信装置に格納されているチャンネル契約関連情報を更新する必要がある。このため、当該受信装置に確実に契約関連情報を受信させる仕組みが必要であり、送信される地域を限定することにより頻繁に契約関連情報を送信可能とした本実施の形態は極めて有用である。

【0142】なお、本実施の形態においても、図1及び図21の実施の形態で述べた種々の変形を同様に構成可能である。

【0143】

【発明の効果】以上説明したように本発明によれば、限定受信に必要な情報の放送を効率化することにより、送信量の増大を抑制することができるという効果を有する。

【図面の簡単な説明】

【図1】本発明に係る限定受信システムの一実施の形態を示す説明図。

【図2】コンテンツパケットのパケット形式を示す説明図。

【図3】番組関連情報パケットのパケット形式を示す説明図。

【図4】契約関連情報パケットのパケット形式を示す説明図。

【図5】ワーク鍵情報の形式を示す説明図。

【図6】チャンネル契約関連情報を示す説明図。

【図7】受信装置の全体構成を示すブロック図。

【図8】受信装置の作用を説明するためのフローチャート。

【図9】受信装置の作用を説明するためのフローチャート。

【図10】受信装置の作用を説明するためのフローチャート。

【図11】受信装置の作用を説明するためのフローチャート。

【図12】広域放送局1内に設けられた広域局契約管理装置40の具体的な構成を示すブロック図。

【図13】図12中の契約ユーザDB42に蓄積されている情報のフォーマットを示す説明図。

【図14】図12中の地域局DB43に蓄積されている情報のフォーマットを示す説明図。

【図15】図12中のワーク鍵DB46に蓄積されている情報のフォーマットを示す説明図。

【図16】地域局送信用契約関連情報を示す説明図。

【図17】図1中の地域局3, 4, …に設けられる地域局契約管理装置50の具体的な構成を示すブロック図。

【図18】実施の形態の動作を説明するためのフローチャート。

【図19】実施の形態の動作を説明するためのフローチャート。

【図20】実施の形態の動作を説明するためのフローチャート。

【図21】本発明の他の実施の形態を示す説明図。

【図22】図21中の広域局61に設けられる広域局契約管理装置71の具体的な構成を示すブロック図。

【図23】地域局送信用契約関連情報を示す説明図。

【図24】図21中の地域局62, 63, …に設けられる地域局契約管理装置81の具体的な構成を示すブロック図。

【図25】実施の形態の動作を説明するためのフローチャート。

【図26】階層構造を利用した実施の形態を示す説明図。

【図27】図27は鍵構成を示す説明図。

【図28】図28は契約関連情報パケットを示す説明図。

図。

【図29】図29は契約関連情報を示す説明図。

【図30】図30は受信装置の構成を示すブロック図。

【図31】受信装置の動作を説明するためのフローチャート。

【図32】受信装置の動作を説明するためのフローチャート。

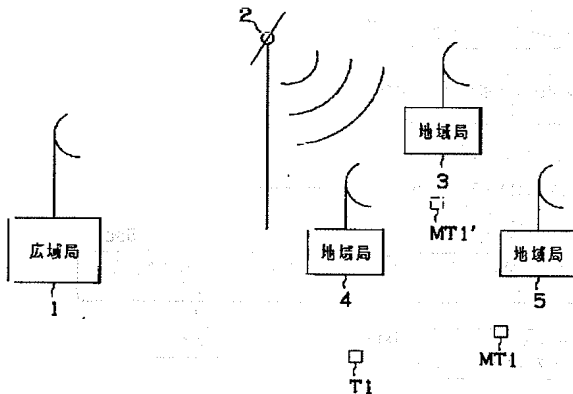
ート。

【図33】受信装置の動作を説明するためのフローチャート。

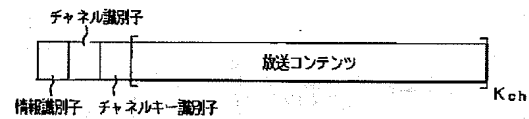
【図34】デジタル放送において採用される限定受信を可能にする鍵構成の一例を示す説明図。

1…広域局、2…衛星、3～5…地域局。

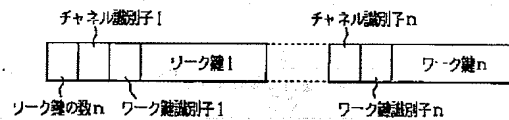
【図1】



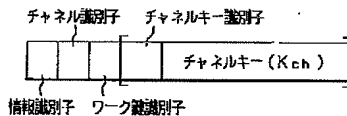
【図2】



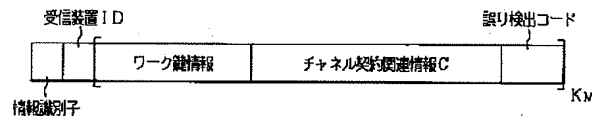
【図5】



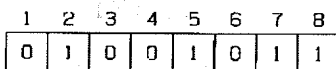
【図3】



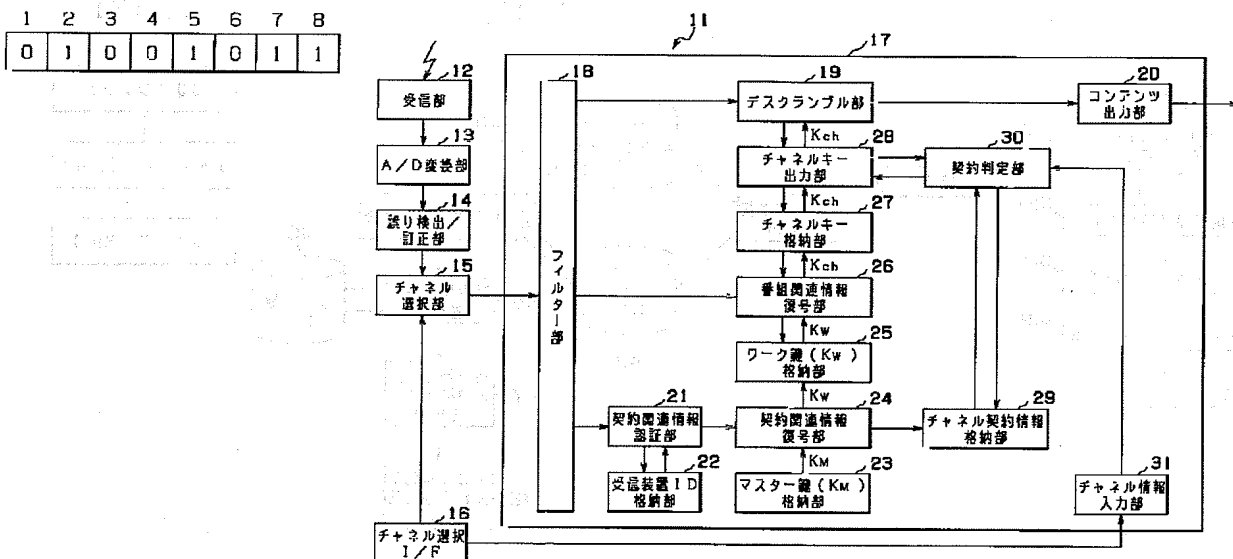
【図4】



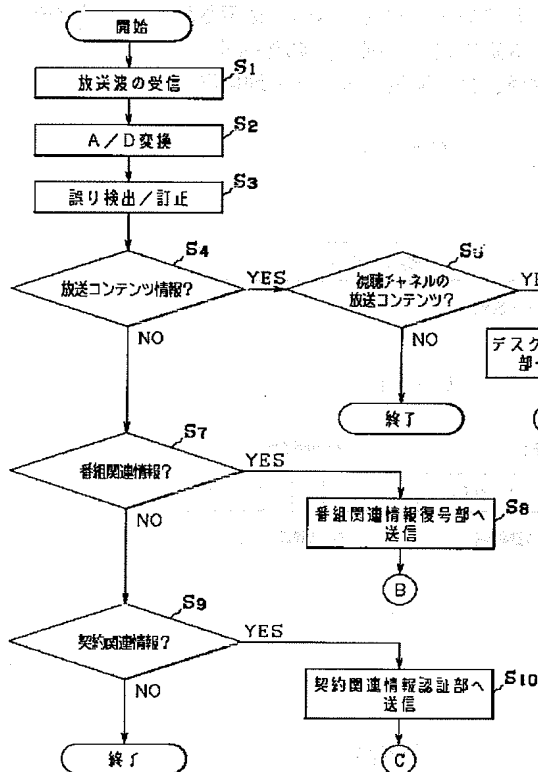
【図6】



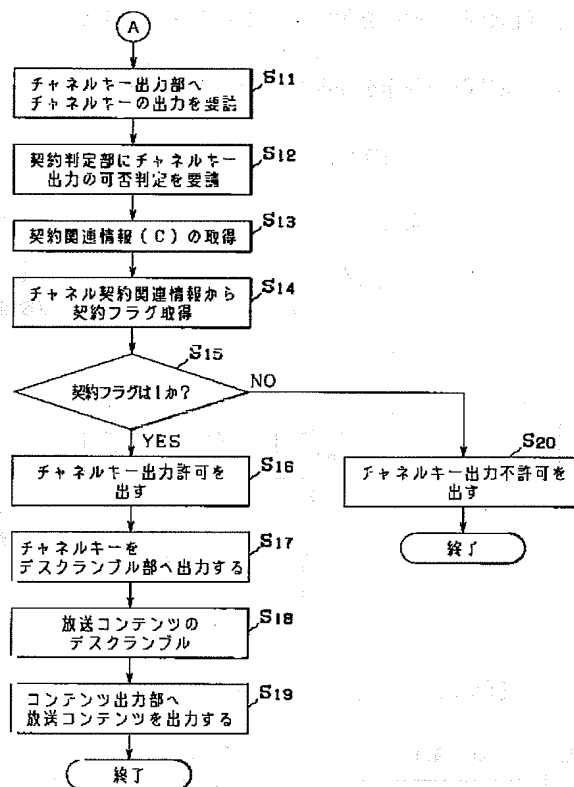
【図7】



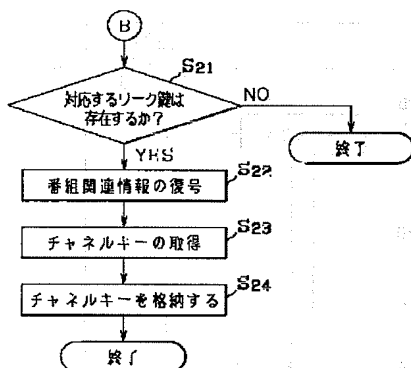
【図8】



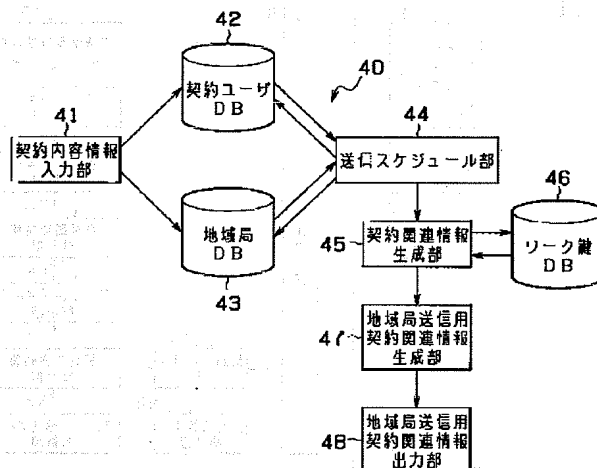
【図9】



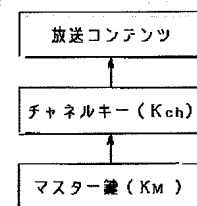
【図10】



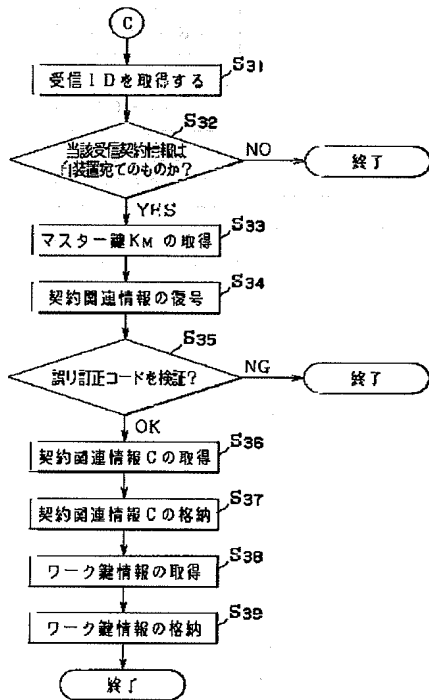
【図12】



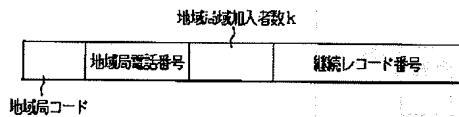
【図27】



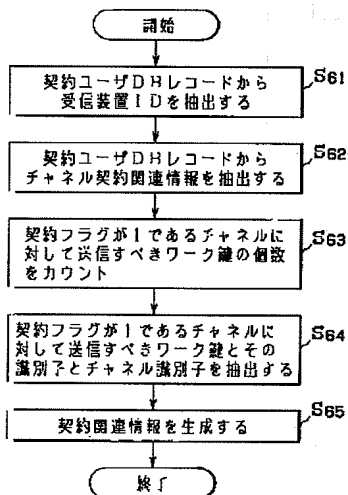
【図11】



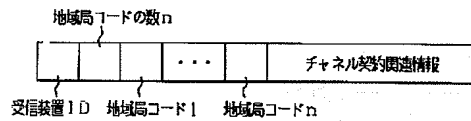
【図14】



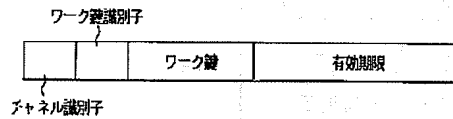
【図19】



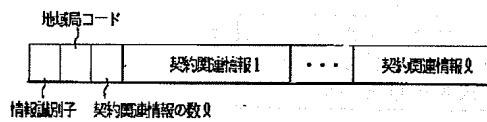
【図13】



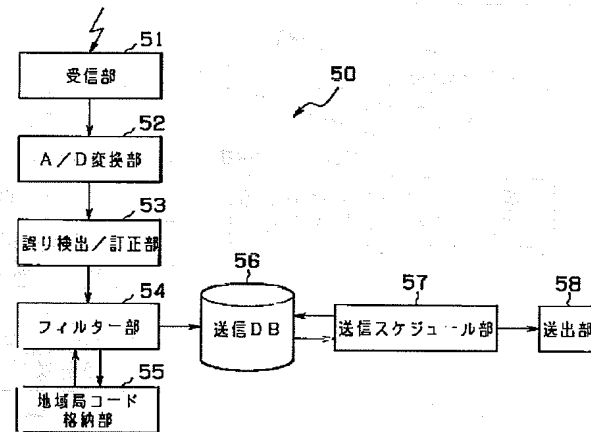
【図15】



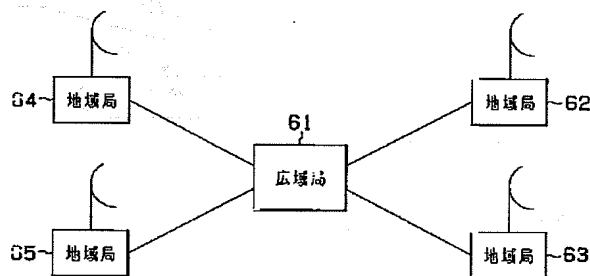
【図16】



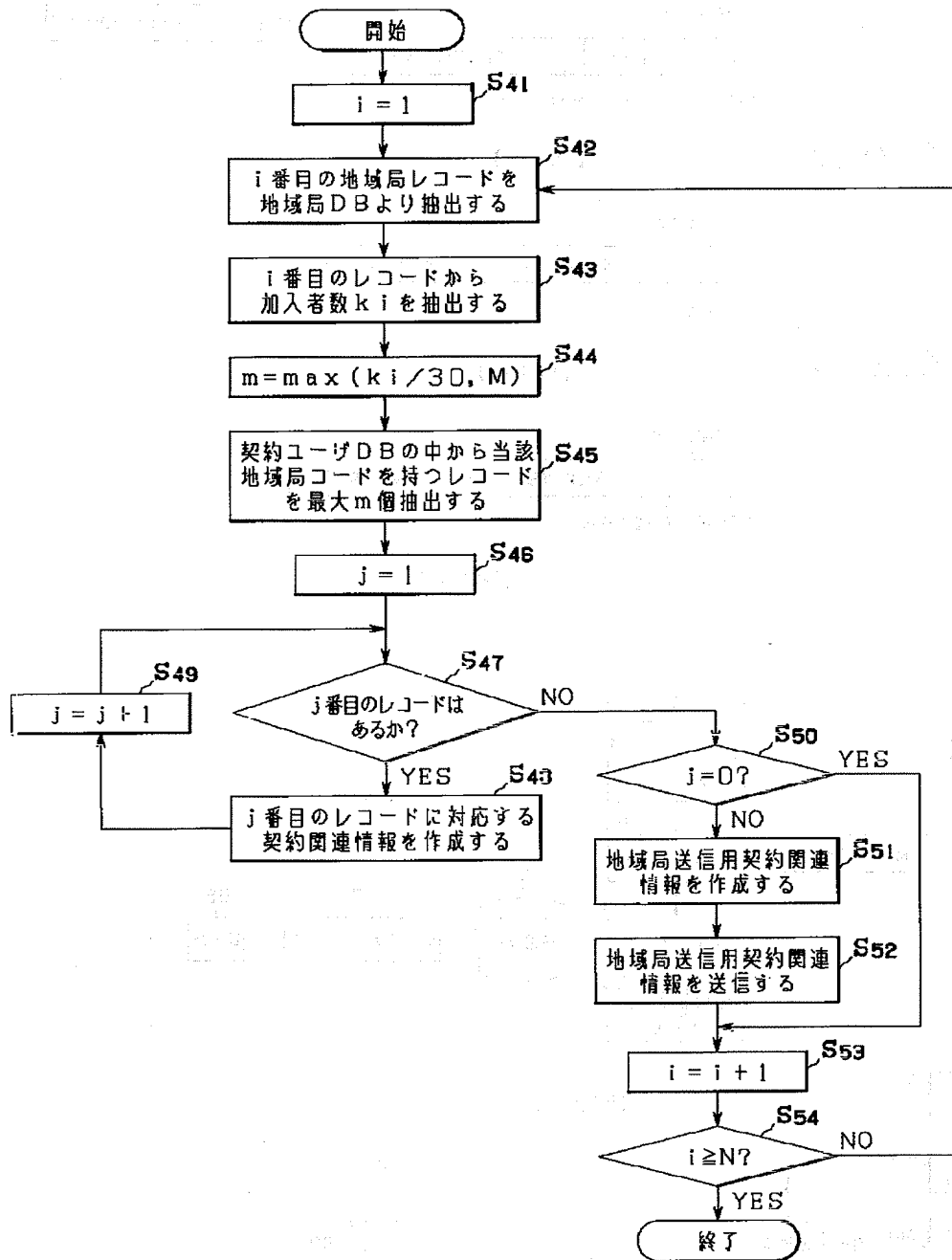
【図17】



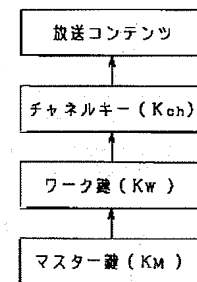
【図21】



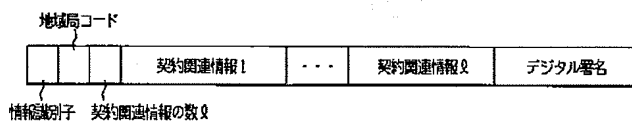
【図18】



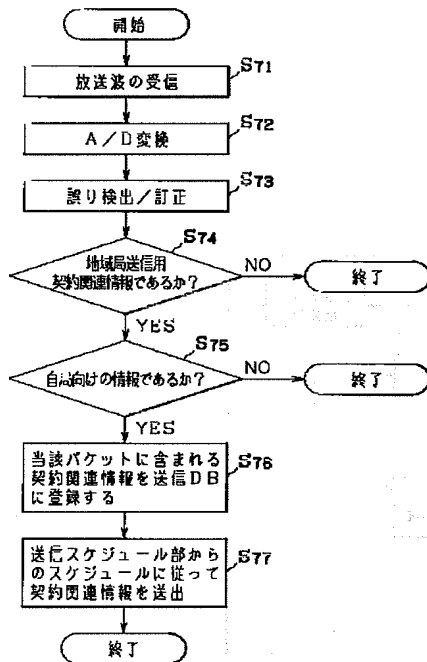
【図34】



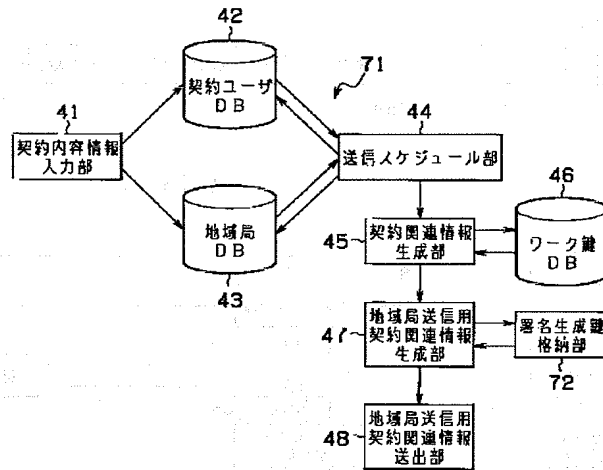
【図23】



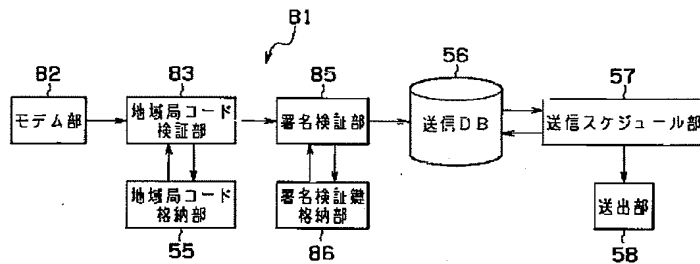
【図20】



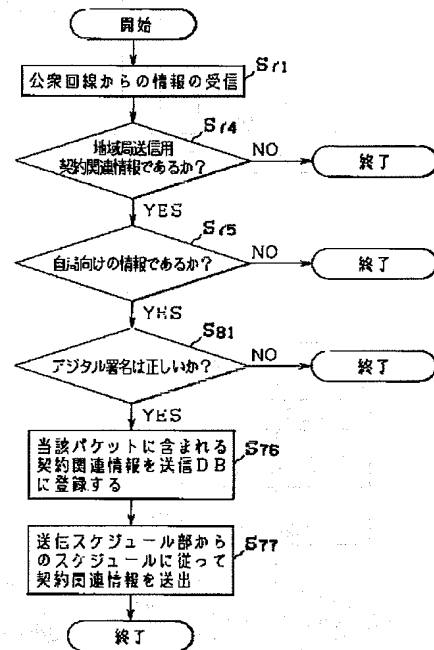
【図22】



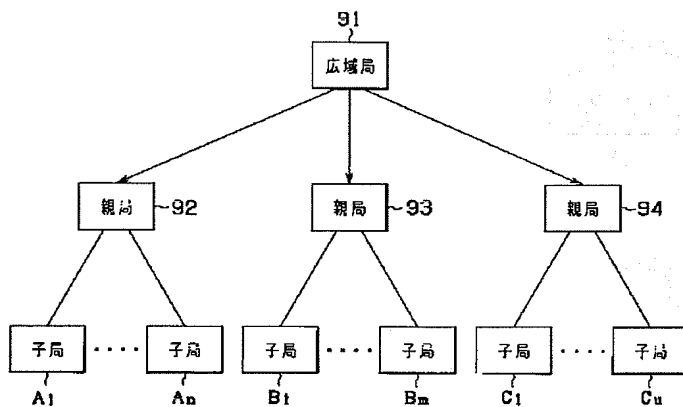
【図24】



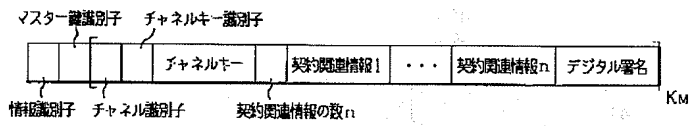
【図25】



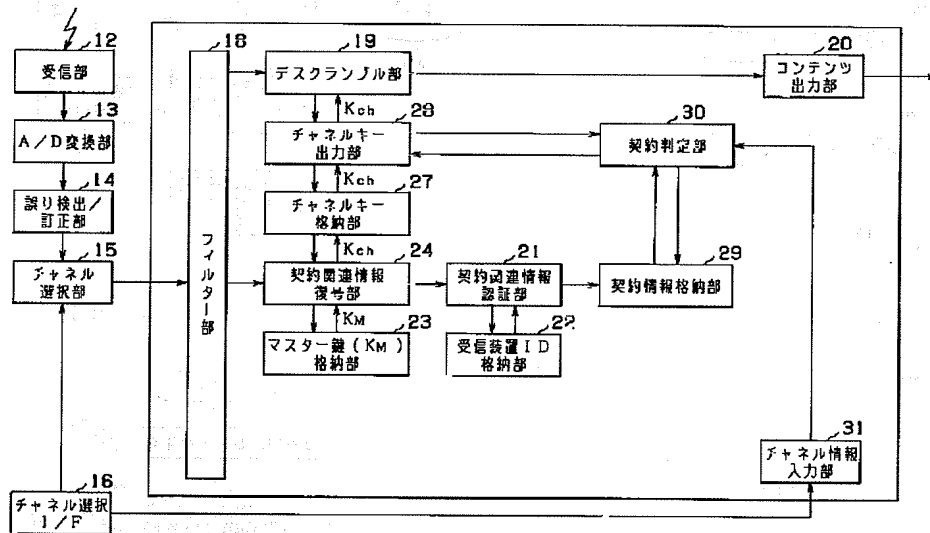
【図26】



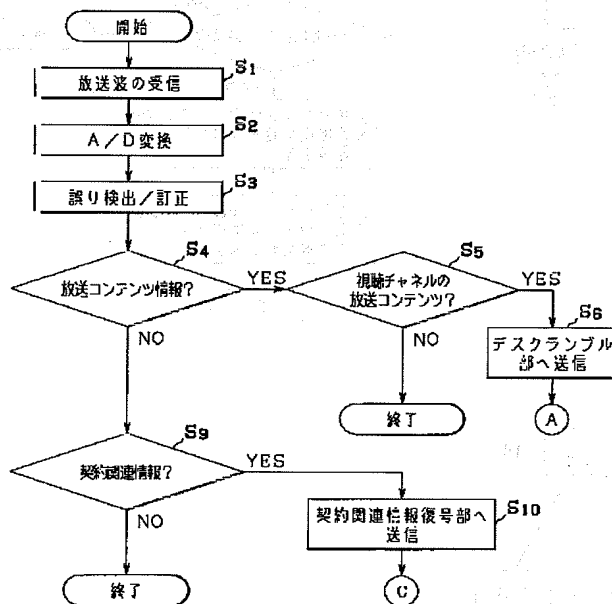
【図28】



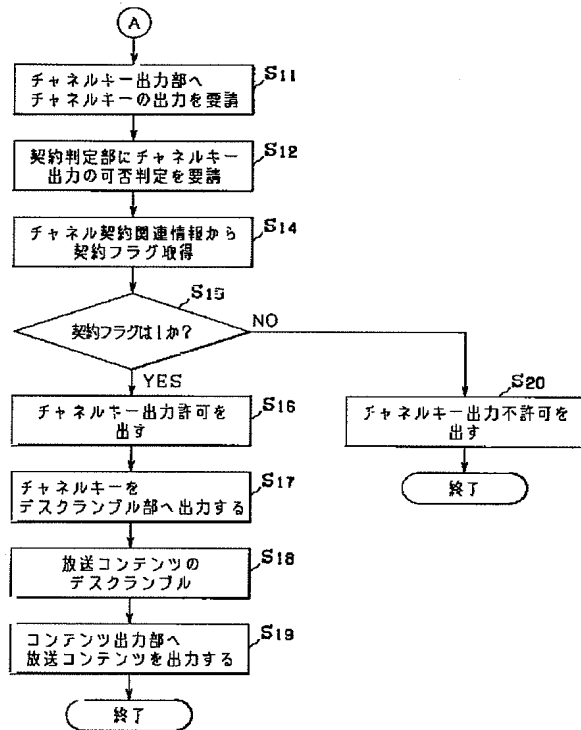
【図30】



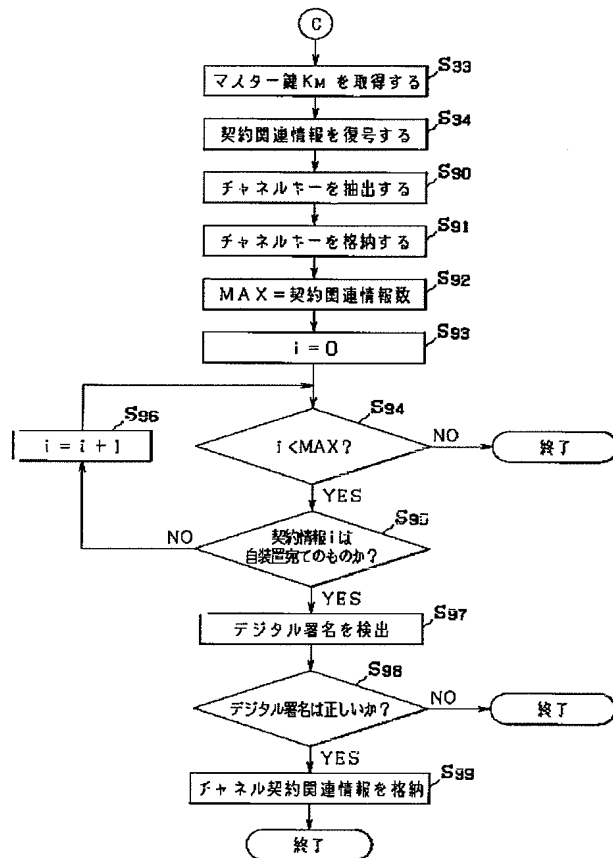
【図31】



【図32】



【図33】



フロントページの続き

(51)Int. Cl.⁷

識別記号

F I

H 0 4 L 9/00

6 0 1 E

(参考)

Fターム(参考) 5C064 BA01 BB02 BB07 BC07 BC17
 BC22 BD07 BD08
 5J104 AA04 AA07 AA09 AA16 BA03
 EA06 EA18 EA26 KA02 NA02
 NA03 NA42 PA05